UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

ALP BAYSAL, THOMAS MAXIM, and SANDRA ITALIANO individually and on behalf of all others similarly situated, Plaintiffs, v. MIDVALE INDEMNITY COMPANY and AMERICAN FAMILY MUTUAL INSURANCE COMPANY, S.I., Defendants.	Civil Action No. 3:21-cv-00394-wmc **AMENDED COMPLAINT -- CLASS ACTION** **JURY DEMAND**

Plaintiffs Alp Baysal, Thomas Maxim, and Sandra Italiano individually, and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against Defendants Midvale Indemnity Company and American Family Insurance Company, S.I. and allege as follows:

I. INTRODUCTION

1. Every year millions of Americans have their most valuable personal information stolen and sold online because of unauthorized data disclosures. Despite warnings about the severe impact of unauthorized data disclosures on Americans of all economic strata, companies still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data about their customers or potential customers.

2. Defendants Midvale Indemnity Company ("Midvale") and American Family Mutual Insurance Company, S.I. ("American Family") (collectively, "Defendants") provide insurance products, including car insurance, to Americans across the country. Midvale is a subsidiary of American Family. Midvale promises to "protect the confidentiality of the information that we have about you by restricting access to those employees who need to know that information to provide our products and services to you. We maintain physical electronic and procedural safeguards that comply with federal and state regulations to guard your information."[1] American Family "recognize[s] the importance of our customers' trust. Keeping personal information confidential is a top priority for all American Family Insurance employees, agents and staff."[2]

3. Defendants failed to meet these promises and their obligations to protect the sensitive personal information obtained by them: Defendants readily provided Plaintiffs' and putative Class Members' driver's license number to *anyone* who entered a person's name, address and/or date of birth into their on-line quoting system. Thus, customers, prospective customers, and even members of the public who were not even a prospective customer of Defendants, had this sensitive personal information compromised.

4. Defendants provide "online automobile insurance quotes to consumers through the amfam.com website. To make the quoting process easier for consumers, an American Family third-party supplier prefills certain information in the online quoting

[1] https://go.midvaleinsurance.com/privacy-policy/ (last visited June 11, 2021).
[2] https://www.amfam.com/privacy-security (last visited June 11, 2021).

form (such as driver's license number) after a consumer enters personal information into the form."[3] Midvale does the same through the midvaleinsurance.com website.[4]

5. As reported by both Midvale and American Family on May 13, 2021, between February 6, 2021 and March 19, 2021 (for American Family customers) and between January 19 and 29, 2021 (for Midvale customers) Defendants "believe unauthorized parties may have used an automated bot process to obtain" Plaintiffs' "driver's license number by entering personal information (such as your name and address) they acquired from unknown sources into a Midvale quoting platform."[5] This means that for an unknown period of time between at least January 19 and March 19, 2021, Plaintiffs' and Class Members' drivers' license numbers were essentially *publicly available* to anyone on various Defendants' online platforms due to Defendants' lax security practices.

6. According to its disclosures to the New Hampshire Attorney General, "On March 18, 2021, American Family was notified by our prefill supplier of a spike in activity on the amfam.com quoting platform between March 1, 2021 and March 7, 2021. We suspected that the spike was associated with unauthorized automated bot activity . . . In response, our CyberFusion Center immediately contained the Incident by taking the

[3] https://www.doj.nh.gov/consumer/security-breaches/documents/american-family-mutual-insurance-20210511.pdf (last accessed June 11, 2021).
[4] *See* https://go.midvaleinsurance.com/start-quote/ (last accessed June 11, 2021).
[5] https://oag.ca.gov/system/files/2021%20Midvale%20Consumer%20Notification%20Ltr%20FINAL.pdf (last accessed June 11, 2021); *see also* https://www.iowaattorneygeneral.gov/media/cms/5132021_American_Family_Insurance_663471B843C3D.pdf (near identical statement regarding American Family platform).

platform offline on March 19, 2021. Subsequent investigation and monitoring identified excessive quote prefill orders dating back to February 6, 2021."[6]

7. American Family reported that "283,734 unique driver's license numbers were returned in the prefill information for all quotes that were generated during" the period, and an additional unknown number of Midvale customers' driver's license numbers were also returned in the prefill information for quotes generated.

8. Defendants are legally required to protect the personal information ("PI") they gather from unauthorized access and exfiltration.

9. As a result of Defendants' failure to provide reasonable and adequate data security, Plaintiffs' and the Class Members' PI has been exposed to those who should not have access to it. Plaintiffs and the Class are now at much higher risk of identity theft and for cybercrimes of all kinds, especially considering the highly valuable and sought-after private PI stolen here.

II. PARTIES

10. Plaintiff Alp Baysal is a resident of Brooklyn, New York. On or about May 13, 2021, Plaintiff Baysal received notice from Midvale that Defendants improperly exposed his PI to unauthorized third parties. Plaintiff Baysal never sought a quote for insurance of any sort from Defendants.

11. Plaintiff Thomas Maxim is a resident of Brooklyn, New York. On or about May 13, 2021, Plaintiff Maxim received notice from American Family that Defendants

[6] https://www.doj.nh.gov/consumer/security-breaches/documents/american-family-mutual-insurance-20210511.pdf (last accessed June 11, 2021).

improperly exposed his PI to unauthorized third parties. Plaintiff Maxim never sought a quote of any sort from Defendant.

12. Plaintiff Sandra Italiano is a resident of Burlington, North Carolina. On or about May 13, 2021, she received notice from Midvale that Defendants improperly exposed her PI to unauthorized third parties. Plaintiff Italiano never sought a quote of any sort from Defendant.

13. Defendant Midvale Indemnity Company is a privately held insurance company incorporated in Wisconsin and headquartered in Madison, Wisconsin. Midvale is an insurance provider that is licensed to do business and markets and sells insurance policies in Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania , Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

14. Defendant American Family is a privately held mutual insurance company incorporated in Wisconsin and headquartered in Madison, Wisconsin. American Family is licensed to do business and markets and sells insurance policies in Arizona, Colorado, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Minnesota, Missouri, Nebraska, Nevada, North Dakota, Ohio, Oregon, South Dakota, Utah, Washington, and Wisconsin.

III. JURISDICTION AND VENUE

15. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs. The Court also has federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers' Privacy Protection Act claims and supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

16. This Court has personal jurisdiction over Defendants because they maintain their principal place of business in this District, are registered to conduct business in Wisconsin, and have sufficient minimum contacts with Wisconsin.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendants reside in this District and on information and belief, a substantial part of the events or omissions giving rise to Plaintiffs' and Class Members' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendants Collect PI and Fail to Provide Adequate Data Security.

18. Defendants have sold insurance, including automobile insurance, since 1927 under various named and corporate forms. "The American Family Enterprise is a family of companies dedicated to delivering unparalleled service and exceptional protection to our customers."[7]

[7] https://www.amfam.com/about/mission (last accessed June 11, 2021).

19. Defendants currently offer various types of insurance policies, including vehicle, home, life, renters' and business.[8]

20. Like other insurance providers, both American Family and Midvale have online auto quote platforms available to all persons capable of accessing them via the internet. Visitors to American Family insurance websites can "Get A Quote" instantly after providing personal information.

21. Defendants' quoting feature uses the information entered by the website's visitor, combines it with additional information the system matches, and then automatically pulls information from a third–party to provide the visitor a quote. Defendants contract with a third–party "prefill supplier" that "prefills certain information in the online quoting form (such as driver's license number) after a consumer enters personal information into the form."[9]

22. Unfortunately, Defendants' online quote system was configured to allow anyone with a few basic bits of data to get Defendants' system to auto–fill the remaining information, including driver's license numbers, from their databases, thus allowing virtually anyone to access and view that information.

23. On or around March 18, 2021, Defendants were notified by the third–party prefill supplier that Defendants' instant quote feature had "a spike in activity." Defendants believe the spike in activity was due to hackers using an automated process, or "bot," on

[8] https://www.amfam.com/insurance (last accessed June 11, 2021); https://go.midvaleinsurance.com/company/ (last accessed June 11, 2021).
[9] https://www.doj.nh.gov/consumer/security-breaches/documents/american-family-mutual-insurance-20210511.pdf (last accessed June 11, 2021).

the instant quote feature to obtain the drivers' license numbers and addresses of Plaintiffs and the members of the Class, which includes many people who never applied for insurance with Defendants or were even necessarily aware of Defendants' existence. In other words, Defendants believe hackers obtained the PI that Defendants knowingly and negligently provided public access to via their instant quote feature.

24. This incident is referred to herein as the "Unauthorized Data Disclosure."

25. Plaintiffs Baysal and Italiano, along with members of the Class, received a letter from Midvale titled "Notice of Data Breach," dated May 13, 2021. The letter stated that their PI, detailed below, may have been compromised, and included the following:

> **What Happened**
> We believe unauthorized parties may have used an automated bot process to obtain your driver's license number by entering personal information (such as your name and address) they acquired from unknown sources into a Midvale quoting platform.
>
> We are notifying you because you may have been affected by this incident. If you did not request an insurance quote using a Midvale quoting platform between January 19, 2021 and January 29, 2021, the unauthorized parties may have requested a quote in your name and may have obtained your driver's license number. If, however, you did request a quote from a Midvale quoting platform between January 19, 2021 and January 29, 2021, you are not affected by this incident.
>
> **What Information Was Involved**
> To the extent you were affected by this incident, unauthorized parties may have obtained your driver's license number.
>
> We have reason to believe this data may be used to fraudulently apply for unemployment benefits in your name. Please carefully review any written communications you receive from your state's unemployment agency, especially if you have not applied for unemployment benefits. If you suspect that your data has been used to fraudulently apply for unemployment benefits, you should contact the relevant state unemployment agency immediately.

What We Are Doing

We identified the unauthorized activity and immediately took action to address it. We blocked the activity and worked to notify potentially affected consumers. We take our responsibility to safeguard personal information seriously and we have enhanced our security controls to help prevent this type of incident from reoccurring.

To help protect you, we are offering you **Single Bureau Credit Monitoring*** services free of charge. These services from Cyberscout, an independent outside firm, will provide you with alerts for twelve months from the date of enrollment whenever changes occur to your Experian credit file. The alert is sent to you the same day that the change or update takes place with the credit bureau. To enroll in these services, please log on to https://security.identityforce.com/benefit/amfam and follow the online instructions. When prompted, please provide the following unique code to receive services:

<CODE HERE>

Important *– You must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.*

There was no delay in providing you this notification as a result of a law enforcement investigation.

What You Can Do

If you wish to monitor your own credit report for unauthorized activity, you may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies: Equifax, Experian and TransUnion. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at (877) 322-8228. Additional information on identify theft protection is also provided in the enclosed pages entitled "Information About Identity Theft Protection."

For More Information

We take the security and privacy of your information very seriously and apologize for any inconvenience this incident may have caused. If you have any questions or concerns regarding this matter, please contact

> Cyberscout at 1-855-535-1805, from 9:00 am to 9:00 pm Eastern time Monday through Friday.
>
> Sincerely,
> Chris Szafranski
> Privacy Director
> Midvale Indemnity Company, subsidiary of American Family Mutual Insurance Company, S.I.[10]

26. Plaintiff Maxim and Members of the Class also received a substantially identical letter from American Family titled "Notice of Data Breach," dated May 13, 2021. The letter stated that their PI, detailed below, may have been compromised, and included the following:

> **What Happened**
> We believe unauthorized parties may have used an automated bot process to obtain your driver's license number by entering personal information (such as your name and address) they acquired from unknown sources into the American Family quoting platform.
>
> We are notifying you because you may have been affected by this incident. If you did not request an insurance quote using the American Family quoting platform between February 6, 2021 and March 19, 2021, the unauthorized parties may have requested a quote in your name and may have obtained your driver's license number. If, however, you did request a quote from the American Family quoting platform between February 6, 2021 and March 19, 2021, you are not impacted by this incident.
>
> **What Information Was Involved**
> To the extent you were affected by this incident, unauthorized parties may have obtained your driver's license number.
>
> We have reason to believe this data may be used to fraudulently apply for unemployment benefits in your name. Please carefully review any written communications you receive from your state's unemployment agency,

[10] Midvale's *Notice of Data Breach*, as filed with the California Attorney General, https://oag.ca.gov/system/files/2021%20Midvale%20Consumer%20Notification%20Ltr%20FINAL.pdf (last accessed on June 11, 2021).

especially if you have not applied for unemployment benefits. If you suspect that your data has been used to fraudulently apply for unemployment benefits, you should contact the relevant state unemployment agency immediately.

What We Are Doing
We identified the unauthorized activity and immediately took action to address it. We blocked the activity and worked to notify potentially affected consumers. We take our responsibility to safeguard personal information seriously and we have enhanced our security controls to help prevent this type of incident from reoccurring.

To help protect you, we are offering you **Single Bureau Credit Monitoring*** services free of charge. These services from Cyberscout, an independent outside firm, will provide you with alerts for twelve months from the date of enrollment whenever changes occur to your Experian credit file. The alert is sent to you the same day that the change or update takes place with the credit bureau. To enroll in these services, please log on to https://secure.identityforce.com/benefit/amfam and follow the online instructions. When prompted, please provide the following unique code to receive services:

<CODE HERE>

Important *– You must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.*

There was no delay in providing you this notification as a result of a law enforcement investigation.

What You Can Do
If you wish to monitor your own credit report for unauthorized activity, you may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies: Equifax, Experian and TransUnion. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at (877) 322-8228. Additional information on identify theft protection is also provided in the enclosed pages entitled “Information About Identity Theft Protection.”

> **For More Information**
> We take the security and privacy of your information very seriously and apologize for any inconvenience this incident may have caused. If you have any questions or concerns regarding this matter, please contact Cyberscout at 1-855-535-1805, from 9:00 am to 9:00 pm Eastern time Monday through Friday.
>
> Sincerely, Chris Szafranski
> Privacy Director
> American Family Mutual Insurance Company, S.I.[11]

27. The Notices confirm that Plaintiffs became victims of the Unauthorized Data Disclosure even though they did not have a prior relationship with Defendants and *only* if they *had not* sought an insurance quote from Defendants.

28. After receiving Unauthorized Data Disclosure notice letters, it is reasonable for Plaintiffs and Class Members in this case to believe that the risk of future harm (including identity theft) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. In fact, Defendants' letters acknowledge the harm related to potential fraudulent use of the data—including providing a warning of a specific danger regarding unemployment benefits—and Defendants encourage affected individuals to use the identity theft protection service offered and note that "It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity."[12] This is because the drivers'

[11] American Family's *Notice of Data Breach*, as filed with the Iowa Attorney General, https://www.iowaattorneygeneral.gov/media/cms/5132021_American_Family_Insurance_663471B843C3D.pdf (last accessed on June 11, 2021).
[12] *See supra* nn. 10, 11.

license numbers are taken for the purpose of committing fraud in the name of the person whose license information is taken.

B. The PI Exposed by Defendants as a Result of Their Inadequate Data Security is Highly Valuable on the Black Market.

29. The information exposed by Defendants is very valuable to phishers, hackers, identity thieves and cyber criminals, especially at this time where unprecedented numbers of fraudsters are filing fraudulent unemployment benefit claims.

30. Cybercrime has been on the rise for the past decade and continues to climb exponentially; as of 2013 it was being reported that nearly one out of four data breach notification recipients become a victim of identity fraud.[13]

31. Stolen PI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

32. When malicious actors infiltrate companies and copy and exfiltrate the PI that those companies store or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[14] "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the

[13] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[14] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited May. 29, 2021).

hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015),

33. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PI] belonging to victims from countries all over the world. One of the key challenges of protecting PI online is its pervasiveness. As unauthorized data disclosures in the news continue to show, PI about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[15]

34. The PI of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[16]. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[17].

---

[15] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited June 10, 2021).

[16] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited May 29, 2021).

[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 29, 2021).

35. The information compromised in the Unauthorized Data Disclosure is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Unauthorized Data Disclosure is difficult and problematic, to change— that is, driver's licenses and addresses.

36. Recently, Forbes writer Lee Mathews reported on Geico's similar unauthorized data disclosure wherein the hackers also targeted driver's license numbers, "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[18]

37. National credit reporting company, Experian, blogger Sue Poremba also emphasized the value of driver's license information to thieves and cautioned:

> If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license is one of the most important pieces to keep safe from thieves.[19]

---

[18] Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, (April 20, 2021), *available at*: https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658 (last visited May 29, 2021).

[19] Sue Poremba, *What should I do If My Driver's License Number is Stolen?* (Oct. 24, 2018), *available at*: https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited May 29, 2021).

38. In fact, according to CPO Magazine, which specializes in news, insights and resources for data protection, privacy and cyber security professionals, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email."

39. Drivers' license numbers have been taken from auto-insurance providers by hackers in other circumstances, indicating both that this particular form of PI is in high demand and also that Defendants knew or had reason to know that their security practices were of particular importance to safeguard consumer data.[20]

[20] *See* United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (accessed Apr. 27, 2021) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers' license number Data Disclosure on January 19, 2021); Ron Lieber, *How*

40. Once PI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PI being harvested from the victim, as well as PI from family, friends and colleagues of the original victim.

41. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

42. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendants did not rapidly report to Plaintiffs and Class Members that their PI had been stolen. It took Defendants almost two months to do so.

43. Victims of drivers' license number theft also often suffer unemployment benefit fraud, harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

44. Unauthorized data disclosures facilitate identity theft as hackers obtain consumers' PI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PI to others who do the same.

Identity Thieves Took My Wife for a Ride, N.Y. TIMES (Apr. 27, 2021) (describing a scam involving drivers' license numbers and Progressive Insurance).

C. Defendants Were on Notice of the Sensitivity and Private Nature of the PI They Utilized for Insurance Quotes and Their Duty to Safeguard It.

45. "Insurance companies are desirable targets for cyber attackers because they work with sensitive data."[21] In fact, according to the Verizon 2020 Data Breach Investigations Report there were 448 confirmed data breaches in the financial and insurance industries.[22]

46. Defendants claim: "We safeguard, according to strict standards of security and confidentiality, nonpublic, personal information our customers share with us. 'Nonpublic, personal information' includes your name, address, Social Security number and credit information. We maintain safeguards, physical and electronic, to protect this information. We conduct our business in a manner that keeps personal customer information secure."[23] But those safety and security measures were insufficient. The weakness in Defendants' system allowed access and ability to exfiltrate Plaintiffs and the Class Members' driver's license numbers.

D. Defendants Failed to Comply with Federal Trade Commission Requirements.

47. Federal and State governments have established security standards and issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has

[21] Data Protection Compliance for the Insurance Industry (October 7, 2020), *available at*: https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry (last visited May 29, 2021).
[22] Verizon 2020 Data Breach Investigations Report (2020), available at: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf (last visited May 29, 2021).
[23] https://www.amfam.com/privacy-security (last visited June 11, 2021).

issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

48. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[25] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[26]

49. Also, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[27]

---

[24] *See* Federal Trade Commission, *Start With Security* (June 2015), available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 29, 2021).
[25] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 29, 2021).
[26] *Id.*
[27] Federal Trade Commission, *Start With Security*, *supra* footnote 25.

50. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[28]

51. Through negligence in securing Plaintiffs' and Class Members' PI and allowing the thieves to utilize their instant quote website platform to obtain access and exfiltrate individuals' PI, Defendants failed to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and the Class Members' PI. Defendants' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and violate the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801.

E. Plaintiffs' Injuries—Attempts to Secure PI After the Disclosure.

52. Defendants admitted there was unauthorized access to Plaintiffs' and Class Members' PI in the Notice letter and recognized that unauthorized access created imminent harm to Plaintiffs and Class Members because Defendants offered a year of credit monitoring. Plaintiffs and Class Members have been, and will continue to be, injured

[28] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Jan. 8, 2021).

because they are now forced to spend time monitoring their credit, guarding against identity theft, and resolving fraudulent claims and charges because of Defendants' actions and/or inactions.[29]

53. Plaintiff Baysal received a notice from Defendants dated May 13, 2021 ("Notice Letter"). The Notice Letter informed him of the Unauthorized Data Disclosure, stating "[w]e believe unauthorized parties may have used an automated bot process to obtain your driver's license number."[30] The notice also specified: "We have reason to believe this data may be used to fraudulently apply for unemployment benefits in your name."

54. Following the Unauthorized Data Disclosure, in April 2021, Plaintiff Baysal received notice from the New York State Department of Labor that a claim for unemployment insurance benefits was filed using his identity.

55. Upon receiving notice of the above, and the Notice Letter from Defendants, Plaintiff spent time researching his options to respond to the theft of his driver's license, and the use of same to commit identity fraud. Plaintiff spent time contacting the New York State Department of Labor to deal with the fraudulent application of unemployment insurance benefits.

56. He spent and continues to spend additional time reviewing his credit monitoring service results and reports from other online resources concerning the security

[29] Time spent "resolving fraudulent charges and protecting oneself against future identity theft" are injuries and provide Article III standing. *Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688, 696 (7th Cir. 2015).
[30] Plaintiff Baysal's Notice of Data Breach is from Midvale Indemnity Company.

of his identity and financial information. This is time Plaintiff otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

57. Additionally, Plaintiff Baysal has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. He deletes any and all unencrypted, non-password protected electronic documents containing his PI and destroys any documents that contain any of his PI, or that may contain any information that could otherwise be used to compromise his PI.

58. Plaintiff Baysal suffered actual injury from having his PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) identity fraud; (b) loss of his privacy; and (c) imminent and impending further injury arising from the increased risk of fraud and identity theft.

59. As a result of the Unauthorized Data Disclosure, Plaintiff Baysal was a victim of identity theft, and will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

60. Plaintiff Maxim received a notice from Defendants dated May 13, 2021 ("Notice Letter"). The Notice Letter informed him of the Unauthorized Data Disclosure, stating "[w]e believe unauthorized parties may have used an auto.mated bot process to obtain your driver's license number."[31] The notice also specified: "We have reason to

[31] Plaintiff Maxim's Notice of Data Breach is from American Family.

believe this data may be used to fraudulently apply for unemployment benefits in your name."

61. Following the Unauthorized Data Disclosure, in June 2021, Plaintiff Maxim received notice from the New York State Department of Labor that a claim for unemployment insurance benefits was filed using his identity.

62. In August 2021, Plaintiff Maxim also received a letter from Charles Schwab regarding a brokerage account opened in his name. Plaintiff Maxim did not open any account with Charles Schwab.

63. Also, in August 2021, Plaintiff Maxim checked his credit report and discovered a soft inquiry from Klarna on July 30, 2021 that involved an unauthorized purchase from Foot Locker. He also discovered that a new phone number was added to his credit report that was not his.

64. Upon receiving notice of the above, and the Notice Letter from Defendants, Plaintiff spent time researching his options to respond to the theft of his driver's license, and the use of same to commit identity fraud. Plaintiff spent time contacting the New York State Department of Labor to deal with the fraudulent application of unemployment insurance benefits. Plaintiff also spent time contacting Charles Schwab regarding the fraudulently opened account in his name. Further, he spent time contacting Klarna and Foot Locker regarding the unauthorized purchase made in his name and contacting the credit bureaus to remove inaccurate information from his credit report regarding the same.

65. He spent and continues to spend additional time reviewing his credit monitoring service results and reports from other online resources concerning the security

of his identity and financial information. This is time Plaintiff Maxim otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

66. Additionally, Plaintiff Maxim has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. He deletes any and all unencrypted, non-password protected electronic documents containing his PI and destroys any documents that contain any of his PI, or that may contain any information that could otherwise be used to compromise his PI.

67. Plaintiff Maxim suffered actual injury from having his PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) identity fraud; (b) loss of his privacy; and (c) imminent and impending further injury arising from the increased risk of fraud and identity theft.

68. As a result of the Unauthorized Data Disclosure, Plaintiff Maxim was a victim of identity theft, and will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

69. Plaintiff Italiano received a notice from Defendants dated May 13, 2021 ("Notice Letter"). The Notice Letter informed her of the Unauthorized Data Disclosure, stating "[w]e believe unauthorized parties may have used an automated bot process to obtain your driver's license number."[32] The notice also specified: "We have reason to

[32] Plaintiff Italiano's Notice of Data Breach is from Midvale Indemnity Company.

believe this data may be used to fraudulently apply for unemployment benefits in your name."

70. Upon receiving the Notice Letter from Defendants, Plaintiff Italiano spent time researching her options to respond to the theft of her driver's license number. Plaintiff Italiano contacted the Florida Reemployment Assistance Program to notify them that she was a victim of a data breach and to place a fraud alert to mitigate the unauthorized application of unemployment benefits in her name.

71. She spent and continues to spend additional time reviewing her credit monitoring service results and reports from other online resources concerning the security of her identity and financial information. This is time Plaintiff Italiano otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

72. Additionally, Plaintiff Italiano has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. She deletes any and all unencrypted, non-password protected electronic documents containing her PI and destroys any documents that contain any of her PI, or that may contain any information that could otherwise be used to compromise her PI.

73. Plaintiff Italiano suffered actual injury from having her PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) identity fraud; (b) loss of her privacy; and (c) imminent and impending further injury arising from the increased risk of fraud and identity theft.

74. As a result of the Unauthorized Data Disclosure, Plaintiff Italiano will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

F. Plaintiffs and Class Members Suffered Additional Damages.

75. Plaintiffs and Class Members are at risk for actual identity theft in addition to all other forms of fraud.

76. The ramifications of Defendants' failure to keep individuals' PI secure are long lasting and severe. Once PI is stolen, fraudulent use of that information and damage to victims may continue for years.[33]

77. The PI belonging to Plaintiffs and Class Members is private, valuable and is sensitive in nature as it can be used to commit a lot of different harms in the hands of the wrong people. Defendants failed to obtain Plaintiffs and Class Members' consent to disclose such PI to any other person as required by applicable law and industry standards.

78. Defendants' inattention to the possibility that anyone, especially thieves with various pieces of individuals' PI, could obtain any individual's PI by utilizing Defendants' front-facing instant quote platform left Plaintiffs and Class Members with no ability to protect their sensitive and private information.

[33] *2014 LexisNexis True Cost of Fraud Study*, (August 2014), *available at*: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last visited May 29, 2021).

79. Defendants had the resources necessary to prevent the Unauthorized Data Disclosure, but neglected to adequately implement data security measures, despite their obligations to protect PI of Plaintiffs and Class Members from unauthorized disclosure.

80. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into their systems and, ultimately, the theft of PI.

81. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Unauthorized Data Disclosure on their lives.

82. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[34]

83. As a result of Defendants' failures to prevent the Unauthorized Data Disclosure, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

[34] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited May 29, 2021).

a. The compromise, publication, theft, and/or unauthorized use of their PI,

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PI, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fails to undertake appropriate measures to protect the PI in their possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Unauthorized Data Disclosure for the remainder of the lives of Plaintiffs and Class Members.

84. In addition to a remedy for the economic harm, Plaintiffs and the Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further misappropriation and theft.

85. To date, other than providing 12 months of credit monitoring and identity protection services, Defendants do not appear to be taking any measures to assist Plaintiffs and Class Members other than simply telling them to do the following:

- "regularly review statements from your accounts"
- "periodically obtain your credit report"
- "remain vigilant with respect to viewing your account statements and credit

reports"

- obtain a copy of a free credit report
- contact the FTC and/or the state Attorney General's office to obtain additional information about avoiding identity theft

None of these recommendations, however, require Defendants to expend any effort to protect Plaintiffs' and Class Members' PI. It is also not clear that Defendants have made any determination that the credit monitoring and identity protection services are designed or adequate to ameliorate the specific harms of having an exposed driver's license number and address.

86. Defendants' failure to adequately protect Plaintiffs' and Class Members' PI has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Instead, as Defendants' Notice indicates, they are putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

87. Defendants' offer of 12 months of identity monitoring and identity protection services to Plaintiffs and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PI is acquired and when it is used.

G. Defendants' Delay in Identifying and Reporting the Breach Caused Additional Harm.

88. Between January 2021 through February 2021, Plaintiffs' and the Class Members' PI was improperly exposed by Defendants and stolen by hackers. Defendants discovered the Unauthorized Data Disclosure by March 2021, but it was not until two months later that Defendants began notifying those affected by the Unauthorized Data Disclosure, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Unauthorized Data Disclosure.

89. As a result of Defendants' delay in detecting and notifying Plaintiffs and Class Members of the Unauthorized Data Disclosure, the risk of fraud for Plaintiffs and Class Members was driven even higher, and Plaintiffs were unaware of the Unauthorized Data Disclosure when they were victimized by it.

CLASS ACTION ALLEGATIONS

90. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Nationwide Class (the "Class") as defined as follows:

> Nationwide Class: All persons in the United States whose PI was compromised in the Unauthorized Data Disclosure announced by Defendants on or near May 14, 2021.

91. Excluded from the proposed Class are any officer or director of Defendants; any officer or director of any affiliate, parent, or subsidiary of Defendants; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

92. **Numerosity.** Members of the proposed Class likely number in at least the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendants' own records.

93. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein,

b. Whether Defendants' inadequate data security measures were a cause of the Unauthorized Data Disclosure,

c. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PI,

d. Whether Defendants' online quote system auto-populated prospective quotes with PI obtained from the records of Defendants or third parties without the permission or consent of Plaintiffs and the Class,

e. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the data security breach,

f. Whether Defendants violated the Drivers' Privacy Protection Act, 18 U.S.C. § 2724,

g. Whether Plaintiffs and the Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief, and

h. Whether Plaintiffs and the Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

94. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

95. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. All Class Members were subject to the Unauthorized Data Disclosure and had their PI accessed by, used and/or disclosed to unauthorized third parties. Defendants' misconduct impacted all Class Members in the same manner.

96. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

97. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the Class Members pale compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to

individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Violation of the Drivers' Privacy Protection Act ("DPPA"), 18 U.S.C. § 2724

(On behalf of Plaintiffs and the Nationwide Class)

98. Plaintiffs incorporate the above allegations by reference.

99. DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains." 18 U.S.C. § 2724.

100. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

101. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.'" 18 U.S.C. § 2725(1). Drivers' license numbers are motor vehicle records and personal information under the

DPPA. 18 U.S.C. § 2725(3); *see also Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 943 (7th Cir. 2015).

102. Defendants obtain, use, and disclose motor vehicle records from their customers.

103. Defendants also obtain motor vehicle records directly from state agencies or through resellers who sell such records.

104. Defendants knowingly publish information to the public on their respective free websites: amfam.com and midvaleinsurance.com.

105. Defendants knowingly linked their respective public websites to systems and/or networks storing, maintaining, and/or obtaining Plaintiffs' and Class Members' PI.

106. During the time period up until and including at least March 19, 2021, PI, including drivers' license numbers, of Plaintiffs and Class Members, were publicly available and viewable on Defendants' instant quote webpages and Defendants knowingly both used and disclosed and/or redisclosed Plaintiffs' and Class Members' motor vehicle records and PI to the general public, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

107. As a result of the Unauthorized Data Disclosure, Plaintiffs and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

SECOND CAUSE OF ACTION

Negligence

(On behalf of Plaintiffs and the Nationwide Class)

108. Plaintiffs incorporate the above allegations by reference.

109. Defendants owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining and testing their data security systems to ensure that Plaintiffs' and Class Members' PI in Defendants' possession, or that could be accessed by Defendants, was adequately secured and protected.

110. Defendants owed a duty of care to Plaintiffs and Members of the Class to provide security, consistent with industry standards, to ensure that their systems and networks adequately protected PI they stored, maintained, and/or obtained.

111. Defendants owed a duty of care to Plaintiffs and Members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in having their systems auto-populate online quote requests with private PI without the consent or authorization of the person whose PI was being provided.

112. Unbeknownst to Plaintiffs and Members of the Class, they were entrusting Defendants with their PI when Defendants obtained their PI from other businesses. Defendants had an obligation to safeguard their information and were in a position to

protect against the harm suffered by Plaintiffs and Members of the Class as a result of the Unauthorized Data Disclosure.

113. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PI. Defendants' misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Unauthorized Data Disclosure.

114. Defendants acknowledge their conduct created actual harm to Plaintiffs and Class Members because Defendants offered one year of credit monitoring.

115. Defendants knew, or should have known, of the risks inherent in collecting and storing PI and the importance of adequate security. Defendants knew about —or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

116. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PI of Plaintiffs and Class Members.

117. Because Defendants knew that a breach of their systems would damage thousands of individuals whose PI was inexplicably stored or was accessible, including Plaintiffs and Class Members, Defendants had a duty to adequately protect their data systems and the PI contained and/or accessible therein.

118. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiffs' and Class Members' PI.

119. In engaging in the negligent acts and omissions as alleged herein, which permitted thieves to access Defendants' systems that stored and/or had access to Plaintiffs' and Class Members' PI, Defendants violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce," and the GLB Act. This includes failing to have adequate data security measures and failing to protect Plaintiffs' and the Class Members' PI.

120. Plaintiffs and the Class Members are among the class of persons Section 5 of the FTC and the GLB Act were designed to protect, and the injuries suffered by Plaintiffs and the Class Members are the types of injury Section 5 of the FTC Act and the GLB Act were intended to prevent.

121. Neither Plaintiffs nor the other Class Members contributed to the Unauthorized Data Disclosure as described in this Complaint.

122. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or theft of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of

privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendants' possession (and/or Defendants have access to) and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PI in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PI.

THIRD CAUSE OF ACTION

Declaratory and Injunctive Relief

(Brought by Plaintiffs and the Nationwide Class)

123. Plaintiffs incorporate the above allegations by reference.

124. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

125. As previously alleged, Plaintiffs and Class Members had a reasonable expectation that companies such as Defendant, who could access their PI through automated systems, would provide adequate security for that PI.

126. Defendants owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PI.

127. Defendants still possess PI regarding Plaintiffs and Class Members.

128. Since the Unauthorized Data Disclosure, Defendants have announced few if any changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Unauthorized Data Disclosure to occur and, thereby, prevent further attacks.

129. The Unauthorized Data Disclosure caused actual harm because of Defendants' failure to fulfill their duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendants' failure to address the security failings that lead to such exposure.

130. There is no reason to believe that Defendants' security measures are more adequate now than they were before the Unauthorized Data Disclosure to meet Defendants' legal duties.

131. Plaintiffs, therefore, seek a declaration (1) that Defendants' existing security measures do not comply with their duties of care to provide adequate security, and (2) that to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,

b. Ordering that Defendants engage third–party security auditors and internal personnel to run automated security monitoring,

c. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures,

d. Ordering that Defendants not be permitted to put PI as part of their source code or be otherwise available on their instant quote webpage,

e. Ordering that Defendants not store or make accessible PI in any publicly facing website,

f. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services,

g. Ordering that Defendants conduct regular computer system scanning and security checks; and

h. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a breach.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully request that the Court enter an order:

a. Certifying the proposed Class as requested herein,

b. Appointing Plaintiffs as Class Representative and undersigned counsel as Class Counsel,

c. Finding that Defendants engaged in the unlawful conduct as alleged herein,

d. Granting injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein,

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws,

iii. requiring Defendants to delete, destroy, and purge the personal information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members,

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal information of Plaintiffs and Class Members' personal information,

v. prohibiting Defendants from maintaining Plaintiffs and Class Members' personal information on a cloud-based database,

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring,

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures,

ix. requiring Defendants to conduct regular database scanning and security checks,

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal information, as well as protecting the personal information of Plaintiffs and Class Members,

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

xii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal information,

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal information to third parties, as well as the steps affected individuals must take to protect themselves,

xv. requiring Defendants to design, maintain, and test their computer systems to ensure that PI in their possession is adequately secured and protected,

xvi. requiring Defendants disclose any future data disclosures in a timely and accurate manner; and

xvii. requiring Defendants to provide ongoing credit monitoring and identity theft repair services to Class Members.

e. Awarding Plaintiffs and Class Members damages,

f. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest on all amounts awarded,

g. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

VI. DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themsevles and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Dated: August 30, 2021

/s/ David W. Asp

David W. Asp (MN #344850)
Kate M. Baxter-Kauf (MN #0392037)
Karen Hanson Riebel (MN #0219770)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South
Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
dwasp@locklaw.com
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com

GAYLE M. BLATT
CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
Gayle M. Blatt
gmb@cglaw.com
P. Camille Guerra
camille@cglaw.com
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

Attorneys for Plaintiffs and the putative Class